Anleitung Gruppenarbeit Kryptografie & Kryptoanalyse

Worum geht es?

In dieser Anleitung lernen Sie zu zweit 3 klassische Verschlüsselungsverfahren kennen:

- Caesar
- Substitution
- Vigenère

Ebenfalls machen Sie Bekanntschaft mit zwei Methoden der Kryptoanalyse:

- Brute-Force
- Häufigkeitsverteilung

Wie wird gearbeitet?

Sie bilden zu zweit ein Team. Damit Sie beide ab und zu den Computer bedienen, finden während dieser Gruppenarbeit einige Platzwechsel statt.
Sie werden Nachrichten ver- und entschlüsseln. Damit Sie nicht ihre eigenen Nachrichten entschlüsseln müssen, arbeiten Sie mit einem Partnerteam zusammen. Mit diesem müssen Sie die geheimen Schlüssel austauschen, ihnen Ihre Nachrichten senden und Nachrichten von ihnen empfangen.

Was ist wenn Sie warten müssen?

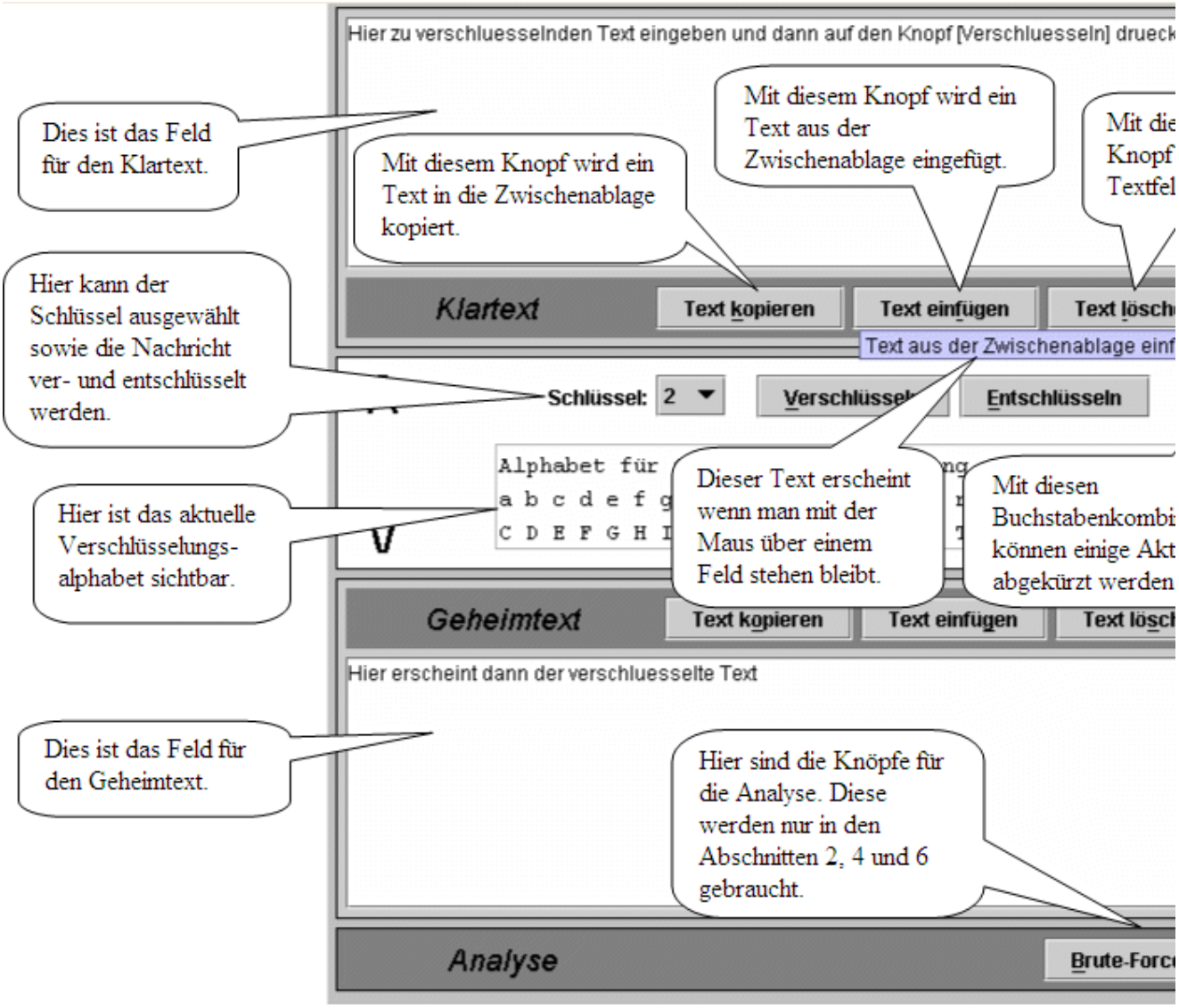
In der Anleitung sind an mehreren Stellen **Links** zu weiterführenden Themen zu finden. Diese erklären zum Teil ein Verschlüsselungsverfahren oder eine Analysemethode genauer oder geben spannende geschichtliche Hinweise. Damit kann die Wartezeit, z. B. auf die Nachricht des Partnerteams, gut genutzt werden.

Fragen?

Im Text hat es ein paar Verständnisfragen. Versuchen Sie diese zu zweit zu beantworten. Wenn Sie die Fragen beantworten können, haben Sie das Thema verstanden. Am Ende der Gruppenarbeit werden die Fragen gemeinsam besprochen.

Wie funktionieren die Programme?

Während dieser Anleitung begegnen ihnen 3 ähnliche Programme, welche alle in etwa so aussehen:



1. Ver-/Entschlüsseln mit Caesar

Im Vortrag haben Sie das Caesar-Verfahren kennen gelernt. Ausserdem haben Sie bereits mit Ihrem Partnerteam einen ersten geheimen Schlüssel ausgetauscht. Nun werden Sie eine verschlüsselte Nachricht mit Ihrem Partnerteam austauschen.

1) **Schreiben Sie mit dem Programm „Caesar“ einen kurzen Klartext.**
2) **Verschlüsseln Sie den Text mit dem abgemachten Schlüssel.**
3) **Kopieren Sie die verschlüsselte Nachricht in die Zwischenablage und senden Sie sie von da per E-Mail an Ihr Partnerteam.**
4) **Warten Sie auf die Nachricht Ihres Partnerteams.**

Zum Zeitvertrieb: Die Caesar-Chiffrierung

5) **Entschlüsseln Sie die vom Partnerteam empfangene Nachricht.**

2. Kryptoanalyse des Caesar-Verfahrens

Das Caesar-Verfahren ist schon über 2000 Jahre alt. Es ist deshalb nicht erstaunlich, dass es sehr leicht zu brechen ist. Die Analysemethode nennt sich „Brute-Force“, was nichts anderes heisst als „rohe Gewalt“. Der Trick besteht darin, dass einfach alle möglichen Schlüssel ausprobiert werden, und man schaut, was dabei jeweils als Klartext herauskommt.

Frage:
Wie viele Schlüssel-Möglichkeiten gibt es beim Caesar-Verfahren?

1) **Bevor es losgeht ist ein erster Platzwechsel angesagt: Die Person welche bis anhin den Computer bedient hat wird Zuschauer, und umgekehrt.**
2) **Schreiben Sie mit dem Programm „Caesar“ einen neuen Klartext.**
3) **Verschlüsseln Sie den Text mit einem neuen, dem Partnerteam unbekannten Schlüssel.**
4) **Senden Sie die neue Geheimnachricht an Ihr Partnerteam.**
5) **Warten Sie auf die Nachricht Ihres Partnerteams.**

Zum Zeitvertrieb: Brute-Force Attacke

6) **Knacken Sie die Nachricht mit der Brute-Force-Methode.**

3. Ver-/Entschlüsseln mit Substitution

Irgendwann haben Caesars Nachfahren herausgefunden, dass dieses Verfahren nicht sehr sicher ist. Wenn jedoch die Anzahl der möglichen Schlüssel erhöht werden könnte, dann würde die Kryptoanalyse massiv erschwert werden. Dies gelingt mit dem Substitutionsverfahren. Dabei wird jeder Buchstabe des Klartextes durch einen beliebigen Buchstaben aus dem Geheimtext ersetzt („substituieren“= „ersetzen“). Es werden nicht mehr alle Buchstaben um gleich viele Stellen verschoben wie beim Caesar-Verfahren.

Damit man sich dazu den Schlüssel gut merken kann, geht man folgendermassen vor:
Die Buchstaben des Klartextalphabetes werden der Reihe nach hingeschrieben. Darunter wird zuerst das Schlüsselwort (im Beispiel: „KRYPTO“) geschrieben, und dann kommen der Reihe nach alle im Schlüsselwort nicht benutzten Buchstaben des Alphabetes.

Beispiel mit Schlüsselwort „KRYPTO“:

```
abcdefghijklmnopqrstuvwxyz
KRYPTOABCDEFGHIJLMNQSUVWXZ
```

Damit wird aus dem Klartext „hallo“ der Geheimtext „BKFFI“.

Das Substitutionsverfahren ist ein symmetrisches Verfahren. Deshalb funktioniert die Entschlüsselung wie beim Caesar-Verfahren.

Mit dem Programm „Substitution“ können Sie dieses Verfahren jetzt ausprobieren:

1) **Treffen Sie sich mit Ihrem Partnerteam für einen neuen geheimen Schlüsselaustausch.**
2) **Schreiben Sie einen kurzen Klartext.**
3) **Verschlüsseln Sie die Nachricht.**
4) **Senden Sie die Nachricht an Ihr Partnerteam.**
5) **Warten Sie auf eine Nachricht von Ihrem Partnerteam.**

Zum Zeitvertrieb: Die monoalphabetische Substitution

6) **Entschlüsseln Sie die neue Nachricht mit Hilfe des ausgetauschten Schlüssels.**

Frage:
Was müssen Sie als Schlüssel eingeben, damit trotz vermeintlicher Verschlüsselung keine Verschlüsselung stattfindet?

4. Kryptoanalyse des Substitutionsverfahrens

Das Substitutionsverfahren scheint ziemlich sicher zu sein, gibt es doch theoretisch 26! = 403'291'461'126'605'635'584'000'000 mögliche Schlüssel. Eine Brute-Force-Analyse würde sehr lange dauern. Die Kryptoanalytiker haben aber eine andere Methode gefunden. Sie nennt sich „Häufigkeitsanalyse“:
In jeder Sprache gibt es Buchstaben und Buchstabenpaare die häufiger vorkommen als andere. Zum Beispiel ist der Buchstabe ‚e' in der deutschen wie auch in der englischen Sprache mit Abstand der häufigste.

Das Substitutionsverfahren ist wie das Caesar-Verfahren ein monoalphabetisches Verfahren. Aus einem bestimmten Klartextbuchstaben wird immer der gleiche Geheimtextbuchstabe. Deshalb kann man folgendermassen vorgehen:

1. Man zählt wie oft die einzelnen Buchstaben auftreten.
2. Der Buchstabe, der am häufigsten auftritt, ist wahrscheinlich ein ‚e' (ausser der Text stammt aus dem Roman „**Anton Voyls Fortgang**“ von Georges Perec, darin kommt kein einziges ‚e' vor…).
3. Kommt ein Wort mit nur 2 Buchstaben vor, bei dem der erste Buchstabe wahrscheinlich ein ‚e' ist, so ist der 2. Buchstabe vermutlich ein ‚r'. Begründung: ‚er' ist ein häufiges Bigramm (Buchstabenpaar).
4. Es können auch Häufigkeitsdaten von Trigrammen benutzt werden. Trigramme sind Folgen von 3 Buchstaben.
5. Hat man erst einmal ein paar Buchstaben erraten ist es meist nicht allzu schwierig aus dem Kontext noch weitere Buchstaben zu erraten.

Das Zählen der Buchstaben kann einem der Computer gut abnehmen. Dabei hilft das Programm „Substitution“:

1) **Wechseln Sie bitte zuerst mit Ihrem Partner den Sitzplatz, damit er/Sie den Computer bedienen kann.**
2) **Schreiben Sie einen neuen Klartext. Dieser sollte jetzt mindestens 200 Zeichen umfassen.**
3) **Verschlüsseln Sie den Text mit einem neuen Schlüssel.**
4) **Senden Sie die Nachricht an Ihr Partnerteam.**
5) **Warten Sie auf eine neue Nachricht von Ihrem Partnerteam.**

Zum Zeitvertrieb: Frequenzanalyse

6) **Führen Sie eine manuelle Analyse mit Hilfe der Häufigkeitsverteilung durch. Benutzen Sie die Fakten über die Sprache und die Häufigkeitsverteilung. In den Feldern oben rechts können Sie Ihre Vermutungen für die einzelnen Buchstaben eingeben. Die Änderungen erscheinen dann sofort darunter im Text. Die grün hinterlegten Buchstaben sind noch frei.**

Frage:
Wieso sollte der Text mindestens 200 Zeichen umfassen?

5. Ver-/Entschlüsseln mit Vigenère

Nachdem die Kryptoanalytiker auch das Substitutionsverfahren geknackt hatten, waren die Verschlüsselungsspezialisten wieder gefragt. Solange aus einem Klartextbuchstaben immer der gleiche Geheimtextbuchstabe entsteht kann man immer die Häufigkeitsanalyse anwenden.

So entstand die polyalphabetische Verschlüsselung, bei der aus einem Klartextbuchstaben nicht immer der gleiche Geheimtextbuchstabe wird („poly“ = „viel“). Das bekannteste polyalphabetische Verschlüsselungsverfahren heisst Vigenère und funktioniert folgendermassen:

```
   diesistderklartext
 + keykeykeykeykeykey
   ------------------
   ONDDNREIDCPKLWSPCS
```

Der Schlüssel (hier „key“) wird endlos wiederholt unter den Klartext geschrieben. Danach werden zu den Buchstaben des Klartextes die Buchstaben des Schlüssels hinzuaddiert. So wird aus ‚d’ (4. Buchstabe) plus ‚k’ (11. Buchstabe) ein ‚O’ (4 + 11 = 15. Buchstabe). Eine verschlüsselte Nachricht wird entschlüsselt, indem der Schlüssel vom Geheimtext subtrahiert wird.

Mit dem Programm „Vigenère“ können Sie dieses Verfahren ausprobieren:

1) **Benutzen Sie das gleiche Schlüsselwort wie beim Substitutionsverfahren.**
2) **Schreiben Sie eine kurze Nachricht.**
3) **Verschlüsseln Sie die Nachricht.**
4) **Senden Sie die Nachricht an Ihr Partnerteam.**
5) **Warten Sie auf eine Nachricht von Ihrem Partnerteam.**

Zum Zeitvertrieb: Polyalphabetische Algorithmen

6) **Entschlüsseln Sie die verschlüsselte Nachricht mit dem gleichen geheimen Schlüssel.**

Frage:
Wieso wird beim Programm „Vigenère“ in der Mitte das Alphabet nicht angezeigt?

6. Kryptoanalyse des Vigenère-Verfahrens

Das Vigenère-Verfahren wurde auch als „Le chiffre indéchiffrable“ bezeichnet.

Dies können Sie mit dem Programm „Vigenère“ überprüfen:

1) **Wechseln Sie zum letzten Mal den Platz vor dem Computer.**
2) **Schreiben Sie einen neuen Klartext, wiederum mit mindestens 200 Zeichen.**
3) **Verschlüsseln Sie ihn mit einem neuen Schlüssel.**
4) **Senden Sie die Nachricht an Ihr Partnerteam.**
5) **Warten Sie auf die Nachricht Ihres Partnerteams.**

Zum Zeitvertrieb: Polyalphabetische Verschlüsselung -- Vigenère

6) **Versuchen Sie eine Häufigkeitsanalyse auf dieser Nachricht.**
7) **Testen Sie die automatische Vigenère-Analyse.**

Wenn die verschlüsselte Nachricht des Partnerteams genügend lang war, dann konnte die automatische Analyse den Schlüssel wahrscheinlich knacken.

Fragen:
Wie Sieht die Häufigkeitsverteilung aus?

Wieso klappt die Häufigkeitsanalyse hier nicht?
Wieso ist das Knacken der Nachricht auch bei einer polyalphabetischen Verschlüsselung noch möglich?

Bis auch die anderen Teams soweit sind können Sie sich die Antworten auf diese Fragen überlegen. Auf den folgenden Seiten finden Sie Hinweise:

- **Der Kasiski-Test**
- **Kryptoanalyse - Babbage, Kasiski, Friedman**